North Walsham High School E-Safety Policy

The E-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and child protection.

The E-Safety Policy and its implementation will be reviewed annually.

Who are the schools E-Safety coordinators?

There are 4 members of staff who are responsible for E-Safety. They are:

K King (Senior Designated Professional)

I Winter (Deputy Head teacher)

G O'Connor (ICT Service Manager)

J Jonas (ICT Technician)

What is E-Safety?

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones, games consoles and wireless technology. This document aims to educate pupils and staff about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The safe and effective use of the Internet is an essential life-skill, required by all. However, unmediated Internet access brings with it the possibility of placing users in embarrassing, inappropriate and even dangerous situations.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for children. In addition, there is information on weapons, crime and racism,

access to which would be more restricted elsewhere. Children and young people must also learn that publishing personal information could compromise their security and that of others.

Pupils interact with new technologies such as smart phones and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place young people in danger.

Pupils will be taught how to evaluate Internet content

The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to report unpleasant Internet content both in school and online, e.g. using the CEOP Report Abuse icon.

All students and staff must read and digitally sign the 'ICT Acceptable Use Policy' before using any school ICT resource. This acts as a digital signature which is time stamped and archived. Please ensure you read this regularly to be aware of any changes as technology emerges.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Internet filtering and monitoring

The school Internet access is provided by British Telecom in association with Norfolk County Council. It includes sophisticated filtering and anti-virus protection. There is another layer of control and filtering done in school. The school also uses software that monitors any inappropriate words that appear on the screen or are typed on the keyboard. The LA / School will block/filter access to inappropriate sites. The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor NCC can accept liability for the material accessed, or any consequences of Internet access.

The school ICT Team work hard to ensure that the filtering methods selected are appropriate, effective and reasonable.

Communication

All users are expected to adhere to the generally accepted rules of using the school network. Every time you use a workstation you will need to agree to the school acceptable use policy (AUP). Here is some basic guidance. Parents will be asked to sign and return a consent form

Key points to remember regarding E-Safety

Pupils and staff may only use our approved e-mail system which is NSIX Google.

Pupils must immediately tell a teacher if they receive offensive or inappropriate e-mail.

Pupils must not reveal personal details of themselves or others (including location) in any form of communication, or arrange to meet anyone without specific permission.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Photographs that include pupils must be selected carefully and will not enable individual pupils to be clearly identified. Full names will not be used.

Bullying will not be tolerated in this school. If you are being bullied, threatened, humiliated or made to feel bad in any shape or form, tell a teacher straight away.

Staff must not communicate with pupils or parents using public social networking sites such as Facebook, MySpace, Twitter, etc. Staff are strongly advised to follow our suggested Facebook privacy settings hand out.

The use of mobile phones or similar personal devices on the school grounds is prohibited for pupils.

Staff must not use any device to access social networking sites during the working day unless it is for approved school use.

Staff are encouraged to use remote login to access files from home. Those wishing to work on files offline must use the encrypted memory stick that was provided to them.

If staff or pupils discover an unsuitable site, it must be reported to the ICT Department immediately. Doing so will ensure no action is taken against you for viewing.

Internet traffic, printing and nearly all ICT access can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Personal devices may only be connected to the school network via the guest wireless.

Inappropriate Material

In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should notify a teacher immediately if they experience material that they find distasteful, uncomfortable or threatening.

Copyright

Respect for copyright, trademarks and intellectual property rights, and the correct use of published material must be adhered to Copyright information is summarised towards the end of this document.

E-Mail

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between schools in neighbouring villages and in different continents can be created.

The school will consider how e-mail from pupils to external bodies is presented and controlled.

Important items to remember regarding e-mail

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

Pupils full names will not be used anywhere on the website or blog, particularly in association with photographs.

Written permission from parents or carers will be obtained before images of pupils are electronically published.

Pupils and staff are advised never to give out personal details of any kind which may identify themselves or others and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
Pupils and staff may only use school NSIX Google Mail on the school system.

Pupils must immediately tell a teacher if see anything offensive or disturbing.

Staff to pupil email communication must only take place via a school email address and will be monitored.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

The school will consider how e-mail from pupils to external bodies is presented and controlled.

Publishing photographs, images and work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children.

Pupils' full names will be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs or images of pupils are published

Written permission from adults will be obtained before their names, photographs or images of themselves are published

Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

Mrs Sharpe take overall editorial responsibility and ensure that content is accurate and appropriate.

Social Networking

Social networking is forbidden within school with the exception of the Virtual Learning Environment (VLE) which is Google Apps for Education.
The only exception to this rule is certain school staff who have access to some social media sites for school related business or to assist with safeguarding issues.

Outside school, pupils are advised to place only appropriate photos on any social network space. Pupils should consider how public the information is and ensure your privacy is secured. For example, background detail in a photograph could identify you or your location. All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location. Teachers must not run social network spaces for student unless using the school Virtual Learning Environment (VLE) which is Google Apps for Education.

Pupils, parents and staff will be advised on the safe use of social network spaces.

Pupils will be advised to use nicknames and avatars when using social networking sites.

Pupils must not place personal photos on any social network space provided in the school learning platform without permission.

Other devices

Mobile phones and associated cameras will not be used during school time except as part of an educational activity.

The sending of abusive, offensive or inappropriate material is forbidden.

Games machines including the Sony PlayStation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school use.

Staff should not share personal telephone numbers with pupils and parents. (A school phone will be provided for staff where contact with pupils is required).

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Staff and the E-safety policy

All staff will be given the School E-safety Policy and its importance explained. The E-Safety Policy is permanently on the student and staff desktop.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Norfolk Children's Services can accept liability for the material accessed, or any consequences of Internet access.
The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

Radicalisation and Extremism

Threats we are seeing take many forms, not only the high profile incidents of those travelling to countries such as Syria and Iraq to fight, but on a much broader perspective also. The internet, in particular social media, is being used as a channel, not only to promote and engage, but also as a command structure. Often this promotion glorifies violence, attracting and influencing many people including children and in the extreme cases, radicalising them. Research concludes that children can be trusting and not necessarily appreciate bias that can lead to them being drawn into these groups and adopt these extremist views, and in viewing this shocking and extreme content may become normalised to it This threat is not just from groups, such as Islamic State, but from 'far right' groups also. We are perhaps more familiar with this 'grooming' process and the risks posed to children by older young people and adults who form relationships with children to ultimately abuse them – the process is similar and exploits the same vulnerabilities. The school work in conjunction with the UK Safer Internet Centre to educate children on the dangers and risks associated with this new threat.

Handling E-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the head teacher. Complaints of a child protection nature must be referred to the Senior Designated Professional for Safeguarding and dealt with in accordance with school child protection procedures. Pupils and parents will be informed of the complaints procedure.

Introducing the E-safety policy to pupils

Appropriate elements of the E-Safety policy will be shared with pupils

E-Safety rules will be posted in all networked rooms.

Pupils will be informed that network and Internet use will be monitored.

Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils

Staff and the E-safety policy

All staff will be given the School E-Safety Policy and its importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues**.**

Enlisting parents' support

Parents and carers attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.

Parents and carers will from time to time be provided with additional information on E-safety. We hold an annual Internet Safety event.

Legal guidance for the use of electronic communication

This document is designed to inform users of legal issues relevant to the use of electronic communications. It is not professional advice.
Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes have been enacted through:

- The Sexual Offences Act 2003, which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of a child to under 18 years old.
- The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds.
- The Police and Justice Act 2006 which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.
Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.
It is also an offence for a person in a position of trust to cause a child under 18 to watch a sexual act. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust).

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing, showing or playing (or possessing such material with a view to displaying, publishing or distributing it) material, including visual images or sounds, which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose (in relation to the 1st offence – intent is necessary for the offence of sending a false message). *Children, Families and Education Directorate page 37 April 2007*

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioners Office of the type of processing it administers, and must comply with important data protection principles when processing personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (as amended by the Police and Justice Act 2006)

The Act makes it a criminal offence to: (intent is required)
Gain access to computer files or software without permission (for example using someone else's password to access files).

- Gain unauthorised access, as above, in order to commit a further criminal act (such as fraud).
- Impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

Malicious Communications Act 1988

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is a person's right to control the ways in which their material may be used, preventing others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the authors own creation and the result of some degree of labour, skill or judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection.
The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the authors permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes.
It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also unlawful to adapt or use software without a licence or in ways prohibited by the terms of the software licence.
Infringement of copyright is actionable by the copyright owner and may result in an award of damages, an injunction or some similar relief.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred, or hatred on religious grounds or grounds of sexual orientation by displaying, publishing or distributing material, including visual images or sounds which is threatening, abusive or insulting. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. *Children, Families and Education Directorate page 38 April 2007.*

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person who pursues a course of conduct which amounts to harassment of another and which he knows or ought to know amounts to harassment of the other, is guilty of an offence.
A person whose course of conduct causes another to fear on at least two occasions that violence will be used against him is guilty of an offence, if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. RIPA was enacted to comply with the Human Rights Act 1998.
The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 however permit a degree of monitoring, for example, to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
These Regulations do not, however, permit interception carried out in order to gain access to the content of personal communications sent by employees that do not relate to the employer's business. Monitoring of employees should not be undertaken lightly and reference should be made to the Employment Practices Data Protection Code.

Counter Terrorism and Security Act 2015

The Counter-Terrorism and Security Act will disrupt the ability of people to travel abroad to engage in terrorist activity and then return to the UK, enhance the ability of operational agencies to monitor and control the actions of those who pose a threat, and combat the underlying ideology that feeds, supports and sanctions terrorism.

It is a bill to make provision in relation to terrorism and to make provision about retention of communications data, about information, authority to carry and security in relation to air, sea and rail transport and about reviews by the Special Immigration Appeals Commission against refusals to issue certificates of naturalisation; and for connected purposes.

Who to go to if you have any queries? - Pupils

If you have an immediate issue regarding E-Safety, tell your teacher or report it to one of the school E-Safety coordinators.

For general queries, please see the ICT Department who are available in the Technology Faculty Office (opposite T3 and next to A3)

We are more than happy to help provide guidance and advice on all E-Safety issues.

Who to go to if you have any queries? – Staff

Report to ICT Services or if necessary, your Line Manager.